Приложение 11

к приказу от 9 января 2023 г. №01/23-ПД

УТВЕРЖДАЮ

Генеральный директор

ООО "СК "УЛЫБНИСЬ"

_____ / Калачиков Н.В.

9 января 2023 г.

ИНСТРУКЦИЯ

По действиям персонала во внештатных ситуациях при обработке конфиденциальной информации и персональных данных

1. Общие положения

1.1 Данная инструкция призвана регламентировать порядок действий пользователя информационной системы персональных данных «[ИСПДн]» (далее - ИСПДн), ООО "СК "УЛЫБНИСЬ" (далее в Организации) при возникновении внештатных ситуаций.

1.2 Инструкция утверждается руководителем организации. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн Организации, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

1.3 Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

1.4 Задачей данной Инструкции является определение мер защиты от прерывания и определение действий восстановления в случае прерывания.

1.5 Действие настоящей Инструкции распространяется на всех сотрудников Организации, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

1.6 Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного одного раза в два года.

2. Порядок действий при возникновении аварийной ситуации

2.1 В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн.

2.2 Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в «Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств информационной системы персональных данных»

2.3 В кратчайшие сроки, не превышающие одного рабочего дня, ответственный за обеспечение информационной безопасности, администратор баз данных или другой назначенный ответственным за реагирование сотрудник предпринимает меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. При необходимости привлекаются квалифицированные сотрудники сторонних организаций с целью восстановления работоспособности в кратчайшие сроки.

3. **Уровни реагирования на инцидент**

3.1 При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

3.1.1 Уровень 1 – Незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.

3.1.2 Уровень 2 – Авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:

Отказ элементов ИСПДн и средств защиты из-за:

- повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;
- сбоя системы кондиционирования;
- других физических повреждений элементов ИСПДн, критичных для функционирования всей ИСПДн. 3.1.1

3.1.3 Уровень 3 – Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа.

К катастрофам относятся следующие инциденты:

- пожар в здании;
- взрыв;
- просадка грунта с частичным обрушением здания;
- массовые беспорядки в непосредственной близости от Объекта.

4. **Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций**

4.1 Технические меры

4.1.1 К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

- системы жизнеобеспечения;

- системы обеспечения отказоустойчивости;

- системы резервного копирования и хранения данных;

- системы контроля физического доступа.

4.1.2 Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;

- системы вентиляции и кондиционирования;

- системы резервного питания.

4.1.3 Все критичные помещения Организации (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

4.1.4 Порядок предотвращения потерь информации и организации системы жизнеобеспечения ИСПДн описан в «Порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации».

4.2 Организационные меры

4.2.1 Ответственные за реагирование сотрудники ознакомляют всех сотрудников Организации, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий 3х рабочих дней с момента выхода нового сотрудника на работу.

4.2.2 Должно быть проведено обучение сотрудников Организации, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций.

4.2.3 Сотрудники, ответственные за обеспечение безопасности ИСПДн должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

4.2.4 Ответственность за организацию обучения должностных лиц несет должностное лицо, ответственное за обеспечение безопасности ИСПДн.